2009

Review of Browser Extensions, a Man-in-the-Browser Phishing Techniques Targeting Bank Customers

Nattakant Utakrit
Edith Cowan University

DOI: 10.4225/75/57b4164330df2
Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009

A Review of Browser Extensions, a Man-in-the-Browser Phishing Techniques Targeting Bank Customers

Nattakant Utakrit
School of Computer and Security Science
Edith Cowan University

Abstract

Initially, online scammers (phishers) used social engineering techniques to send emails to solicit personal information from customer in order to steal money from their Internet banking account. Data, such as passwords or bank account details, could be further used for other criminal activities. For instance, the scammers may intend to leave the victim's information behind after they have successfully committed the crime so that the police can suspect the visible evidence as a suspicious criminal. Many customers are now aware of the need to protect their banking details from the phishers by not providing any sensitive information. Recently, phishing attacks have become more sophisticated and targeted to the online banking users. Hence, this paper reviews one form of a current type of phishing attack known as a 'man-in-the-browser'. It specifically focuses on the use of browser extensions, including their operational strategies. Techniques to identify, minimize, and prevent this type of attack are considered. Lastly, the author provides specific advice for the bank customers based on her research interests and experience in online banking security.

Keywords

Phishing, man-in-the-browser, Trojan, add-ons, plugins, browser extensions

INTRODUCTION

Phishing has been first introduced as a use of social engineering technique in which potential victims are convinced to provide their confidential information, such as usernames, passwords, and bank account details, to a return email. The attack is often extended by creating fraudulent web pages to persuade customers to believe that they are on the legitimate banking sites. Once an identity has been submitted through the form provided, the information is been sent to the phisher. There are some other spying techniques that are used to track the user's banking information claimed by Ståhlberg (2007), such as screenshot and video capture, code injection of fraudulent pages or form fields, redirecting website, and keystroke logging. Sometimes, obtaining user's information can be combined with multiple penetrating techniques; for example, using the screenshot and video capture to monitor the user's activity and using the keystroke logging to record passwords or information. Subsequently, a newer and more dangerous facet to phishing technology such as a Trojan horse has been released. It operates by becoming embedded in a user's Internet browser and later steals confidential information and sends it back to the scammer. The Trojan horse is known in an attack form of 'man-in-the-browser'.

MAN IN THE BROWSER VS MAN IN THE MIDDLE ATTACKS

Theoretically, man in the browser (MitB) and man in the middle (MitM) attacks are similar in terms of controlling dataflow between the client and the host computer. However, a man in the middle uses a proxy server that relays traffic and takes place at the application layer between the customer's webpage and the legitimate online banking system (Litan & Allan, 2006) which runs on the traffic stream (RSA, 2008). Conversely, a man in the browser operates on an Internet browser that displays on a user's desktop and controls ingoing and outgoing contents at the system level not on the authentication level on a customer's computer screen.

How does man-in-the-browser operate?

Man in the browser is also called a proxy Trojan or a password pinching Trojan (Leyden, 2008). It combines the use of phishing approaches with a Trojan horse technology, inserted into a customer's browser, to modify, capture, and/or insert an additional information on web pages without the customer's and the host's knowledge (Gühring, 2006; Litan & Allan, 2006; Ståhlberg, 2007).

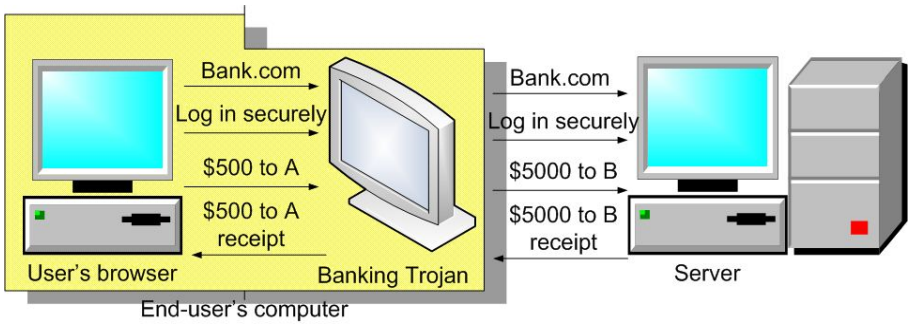


Figure 1- Man-in-the-browser operation

Figure 1 illustrates the process of man-in-the-browser attack. When the Trojan infects the user's computer application or the operating system, it will install an extension program into the browser and wait to be launched next time the browser starts. Whenever the web page is loaded, the Trojan will filter the page based on the list of the targeted sites. If the site is matched with the pattern, the Trojan extension will wait until the user logs in into their bank and starts to transfer the money. When submit button is pressed, the extension will extract data from all fields and modify the value, such as the amount of money and the destination receiver, through the document object model (DOM) interface and resubmit the form to the server. At this stage, the server will not be able to identify whether the values are from the original one or not. Thus, it still performs the normal transaction and generates a receipt back to the Trojan extension, and then the Trojan re-modifies the intended value to display on the user's browser.

In addition, a Trojan can assemble in the Firefox's extension folder or Internet Explorer's extension and activate every time the filtered browser is started (Leyden, 2008). There are various ways that Trojans can be embedded into a customer's computer; for instance, when he or she is viewing an infected email, opening an email attachment, visiting and/or downloading a file from an unsecured website, or even visiting a legitimate website which has been infected with a Trojan (Cronto, 2008). It begins with the establishment of the Trojan application on the hard drive of a user's computer, purposes of injecting itself into a customer's browser. Once the browser is injected, the Trojan malware will wait for the customer to log into their banking website and silently steal money from the customer's account (Ilett, 2006).

How is money stolen?

The Trojan malware will monitor the user's activity on the system and look for data exchanged between a compromised machine and a list of pre-programmed banking sites (Leyden, 2008), then operate its functions when a list of filter strings, which are used to focus on a specific website, is detected (Ståhlberg, 2007). Filter strings can be a URL address and/or a dialogue string such as 'Welcome to the Bank'. The Trojan filter string, such as SilentBanker, is able to mount attacks on over 400 different bank websites worldwide without being detected by two-factor authentication (Cronto, 2008), and the Trojans Bancos.NL have detected 2,764 different bank URLs from over 100 countries (Ståhlberg, 2007).

Browser extension definitions and explosion points

The definitions of the browser extension and its associated features may be defined in various ways. The extension is a small application that provides the additional features to the browsers (Blum & LeBlanc, 2009) and different from an add-on or a plugin (Croll & Power, 2009). The browser extension can be extended into four types covered add-ons, plugins, browser helper objects (BHOs), and unplugs. Vugt (2009, p. 80) explained that the "Add-on is a catch-all term that includes extensions". Pogue (2004, p. 330) added that "An add-on can be any bit of software that beefs up the Web browser." The add-ons are included with alternative themes, and additional language supports. Add-ons affect web pages displayed and how a page is loaded. The add-on applications such as the Video DonwloadHelper captures a video file and saves into a disk, and the Adlock Plus application which can help the users block the advertisements (Vugt, 2009). More example of the add-ons application can be the Greasemonkey (Croll & Power, 2009), ActiveX Controls and the Google toolbar.

Plugins are the unlimited access standalone software which can play an audio file, a show video, or display a document on them. The examples include Java, QuickTime, Windows Media Player, Flash (Croll & Power, 2009), and Adobe Acrobat in which the acrobat can allow the users to read the content of PDF files directly from the browsers (Vugt, 2009).

Browser helper objects (BHOs) are developed by Microsoft Company. They are the browser extensions in-process the component object model (COM) server that the Internet Explorer loaded when it starts up. In other words, BHOs are dynamically loaded libraries (DLL) that run in the address space of the browser and embed the main window of the

browser (Blunden, 2009). BHOs leave registry entries under the registry key `HKLM\SOFTWARE \Microsoft\ Windows\CurrentVersion\Explorer\Browser Helper Objects`. They are written in a variety of programming languages such as C++, used to link IE components to build applications (Microsoft Corporation, 2009). BHOs share a common address space with the browser, and have the greater access to browser resources by enabling a direct reading of browser memory (Louw & Lim, 2008), in order to intercept IE user interactions within the browser process, and store it on a user's computer. They also have merely achieving unlimited access to all resources of the operating systems, such as network sockets, files, and processes (Raffetseder, Kirda, & Kruegel, 2007).

Lastly, some Internet users may occasionally have heard the 'unplug' extension which allows the users to save embedded streaming video content on a webpage, such as YouTube and MySpace, as a video file on a computer (Blum & LeBlanc, 2009).

These extensions are likely to perform malicious activity to capture, modify and steal the customer's banking information and send it back to the attacker via the Internet control message protocol (ICMP) packets, emails or HTTP POST sessions. The malware encodes the data with a simple XOR swap algorithm before placing it into the data section of an ICMP ping packet, which contains captured encoded sensitive data and bypasses administrators and egress filters. Algorithms such as "OR 1=1" in the text field create true conditions to bypass the logic checks or the authentications (Scambray, Shema, & Sima, 2006). These conditions cause the SQL server to return all records from the particular tables, with the consequence that the attacker may gain full access to one or more databases (Rietta, 2006). The packet masquerades as a legitimate traffic, particularly if the keylogger technology has been associated with the Trojan attack (Oiaga, 2006). A man in the browser attack can simply bypass a public key infrastructure (PKI) security measure (Gühring, 2006), a secure socket layer and a transport layer security (SSL/TLS) protocol encryption (Ollmann, 2009). Trojans are very difficult to detect and remove from the system because the network connection is not being related to the Uniform Resource Locator (URL) (Cronto, 2008) as they run on different layers. In addition to transaction authentication, Trojans can circumvent some standard authentication systems that use the PC as a single channel for transmission data to the server as follows:

- Username and password
- Transaction authentication number (TAN)/ Indexed transaction authentication number (iTAN)
- Client certificates
- Secure ID tokens
- One time pad tokens
- Biometry authentication
- Smartcard and/or class 3 reader authentication with client certificates
- Bürgerkarte Security layer
- Digital Signatures with smartcards and class 3 readers (Gühring, 2006)

Tampering techniques with browser extension tools

This paper will review the two most used browsers such as Firefox and Internet Explorer in more detail. Tampering tools masqueraded themselves as a plug-in that is installed on IE and Firefox and have ability to expose aspects of HTTP/HTTPS sessions on the fly, including headers, forms, and cookies (Scambray et al., 2006). Parameters such as GET/POST/PUT can be manipulated or created to send the value changes to any destination without the customer noticing and still return the intended value back to the customer's screen (Ollmann, 2009). Some plug-in Trojans can tamper with the GET parameters, which are used to request a page from a server for a customer (Fadia, 2006), bypass any browser restrictions.

Figure 2 - IE tampering tools (Adapted from Bayden Systems, 2004).

The malware can also tamper with the PUT parameter to access data in the body of the HTTP request that is not accessible from the browser's address bar (Scambray et al., 2006). They may even attack the POST parameter, which is used to upload files to the server through an HTML page not via an FTP service (Fadia, 2006), while a customer is performing an online transaction, a form submission or an online shopping. Figure 2 illustrates how online transaction can be modified. The original price of the laptop was $1995. As soon as the submit order had been pressed, the Trojan extension captured the value with HTTP requests and modified the price of item to become $10. The value in the software contains a number of generated attack strings, such as SQL injection, buffer overflow, cross-site scripting, which can cause problems for web based applications (Bayden Systems, 2004).

Internet Explorer Trojan add-on example

Examples of the add-on browser Trojans include Nuklus.a which collects a certificate from the system certificate storage (Ståhlberg, 2007). As Trojan, Nuklus.a is a browser malware application used for stealing online bank account details, mainly exploited in Internet Explorer (IE.exe). Once the Trojan is installed, it will inject the Trojan's executable file `'taskmang.exe'` (F-Secure Corporation, 2007) which contains the remote address command and the control interface. Therefore, the service system in the victim's computer will be created as:

```
ServiceName = "Taskmng"
DisplayName = "Windows Task Manager"
ImagePath = "%System32%\taskmang.exe"
```
(F-Secure Corporation, 2007)

The Trojan also creates the registry key as an infection marker, the registry sub-key and a system service to run when Windows starts. The following are keys:

```
[HKEY_CLASSES_ROOT\MTBase\"(Default)" = "%System%\mt_32.dll"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Taskmng
```
(SecurityMob, 2007)

Once the attributes and the registry keys have been changed, the Trojan downloads additional components from a remote server using plug-ins and communicates with the control server using HTTP requests which consist of the dynamically loaded libraries (DLLs) files that are loaded by the Trojan using BHOs for IE and/or Firefox. The following table of DLL files includes basic malware plug-ins that may be installed on customers' systems:

Table 1 - Basic dynamically loaded libraries (DLLs) files installed by Trojan browser extensions (F-Secure Corporation, 2007).

DLL File	Description
CertGrabber.dll	Collects certificates from the system certificate storage.
ExeLoader.dll	Executes files.
FFGrabber.dll	Mozilla Firefox HTTP requests sniffer implemented as XML user interface language (XUL) extension module.
IECookieKiller.dll	Removes cookies from the Internet Explorer cache.
IEFaker.dll	Rewrite URLs. The fake addresses are controlled remotely by the attacker.
IEGrabber.dll	IE HTTP request sniffer.
IEMod.dll	Installs as a BHO and allows other modules to hook on Internet connections.
IEScrGrabber.dll	Capture IE screenshots.
IETanGrabber.dll	Redirects internet connections.
NetLocker.dll	Gets/sets a list of system Layered Service Providers (LSP).
ProxyMod.dll	Starts HTTP and Socks proxies on a random port.
PSGrabber.dll	Collects miscellaneous credentials from the system such as email accounts.

These add-ons are installed in the %System%\ directory and automatically start up the next time a customer opens the browser. They can bypass digital signing as they rely on the user opening an executable program file (.exe) by the Windows operating system, not on the default browser installer (.xpi) (Krebs, 2006).

Table 2- Files inserted by Trojan Nuklus.a (ScanSpyware, 2008)

Dynamically loaded libraries (DLLs) files	Registry keys
%systemdir%\mt_32.dll	{3BF77FF3-E054-4728-ADD0-B21EF95EECE1}
IEMod.dll	{24A1E1CC-4393-941E-B765-2264A695D4E3}
IEFaker.dll	{3BF77FF3-E054-4728-ADD0-B21EF95EECE1}
%systemdir%\taskmang.exe	{24A1E1CC-4393-941E-B765-2264A695D4E3}
ProxyMod.dll	{3BF77FF3-E054-4728-ADD0-B21EF95EECE1}
FFGrabber.dll	{24A1E1CC-4393-941E-B765-2264A695D4E3}
IEGrabber.dll	{3BF77FF3-E054-4728-ADD0-B21EF95EECE1}
PSGrabber.dll	{24A1E1CC-4393-941E-B765-2264A695D4E3}
%systemdir%\ExeLoader.dll	Taskmng
%systemdir%\CertGrabber.dll	Taskmng
IEScrGrabber.dll	Taskmng
%systemdir%\IETanGrabber.dll	LEGACY_Taskmng
browsearch.dll	LEGACY_Taskmng
%systemdir%\netd.dll	LEGACY_Taskmng
mshtmllib.dll	
%systemdir%\mscert.dll	
%systemdir%\fdeploy.ocx	
%systemdir%\ptco.dll	
%systemdir%\clfsw.dll	
browserui.dll	
protect.dll	
\out.exe	

Firefox Trojan add-on example

Firefox extensions, written in JavaScript, display on clients' web pages and cannot directly address the browser's memory (Louw & Lim, 2008). A malware author can install the malicious extension software into a user input form or when a web page completes loading. It can record keystrokes, or it can intercept all form data that is being submitted. Furthermore, the extensions can also alter the contents of a page by accessing its DOM representation (Raffetseder et al., 2007). "DOM starts with the browser itself, then the windows and tabs. When you load a page, the browser builds a hierarchy of all the things on the page, such as forms, titles, and headings" (Croll & Power, 2009, p. 299). DOM also contains a browser version and a window size and allows JavaScript to modify the entire webpage where details are stored, such as cookies associates with a site (Croll & Power, 2009). The Trojan that infected in the Firefox extension such as the Trojan.PWS.ChromeInject.A was identified by BitDefender in 2008. It registers itself as an impersonator of the Greasemonkey toolbar and installs into Firefox's add-on directory to search a user's hard drive for the passwords, login details, account information, and the library card numbers (Hruska, 2008). Users can be attacked by opening attachments, accepting ActiveX or JavaScript, or downloading malware-ridden code that attached in the movie (Hruska, 2008). In the directories below are the examples of the file npbasic.dll in the Firefox plug-in folder and the file browser.js

in a firefox chrome folder. They are malware executable plug-in and JavaScript file that install in the Firefox to captures the login information (BitDefender, 2008).

```
%ProgramFiles%\MozillaFirefox\plugins\npbasic.dll
%ProgramFiles%\MozillaFirefox\chrome\chrome\content\browser.js
```

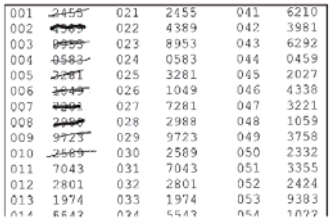
Obviously, malware extensions often attack the Windows registry by inserting the DLL files in the registry keys to then attack the users. Windows registry is a core component of Windows system which stores system preferences, user settings and installed applications. Therefore, if the malware application is installed, it can automatically launch itself at computer start-up. To effectively remove malware extension from Windows registry, all the registry keys and the values associated must be deleted.
Another possible threat from the add-ons attack could occur via Microsoft .NET Framework assistant which exploits the Firefox and the IE on any version and works as an uninstalled mode from the add-on list Firefox (except Windows 7) unless removed from the Windows registry directory (Keizer, 2009). It is installed without user approval. However, Microsoft has released the patches provided in the MS09-054 update to protect the Trojan add-ons. Beside, users could still disable the add-ons in Firefox by selecting Tools>Add-ons>Plugins, selecting Windows Presentation Foundation and clicking Disable.

RISK MITIGATION

Authentication securities, such as virtual keyboards, are still vulnerable to Trojans which can perform a screen or a video capture to bypass them (Ståhlberg, 2007). However, many private security companies are developing applications or tools to prevent man-in-the-browser attacks. Banks may begin to use multi-factor authentications, with separate devices being an option to provide robust defences to shield their customers from man in the browser attacks. These developments are described below.

Anti-man in the browser Trojan technology

Ståhlberg (2007) described how banks and financial organisations can prevent their customers from being attacked by Trojans by monitoring for any anomalous web service access. Banks can also provide their customers with a list of passwords, as shown in Figure 3, so that they may use a random password, and by allowing each password to be used only once. This makes customer authentication of an online banking system more secure.



001	~~2455~~	021	2455	041	6210
002	~~4389~~	022	4389	042	3981
003	~~8953~~	023	8953	043	6292
004	~~0583~~	024	0583	044	0459
005	~~3281~~	025	3281	045	2027
006	~~1049~~	026	1049	046	4338
007	~~7281~~	027	7281	047	3221
008	~~2988~~	028	2988	048	1059
009	~~9723~~	029	9723	049	3758
010	~~2589~~	030	2589	050	2332
011	7043	031	7043	051	3355
012	2801	032	2801	052	2424
013	1974	033	1974	053	9383

Figure 3- A typical one-time password (OTP) scheme used by European banks (Ståhlberg, 2007, p. 2).

TriCipher technology

The TriCipher Armored Credential System (TACS) enhances the device for client authentication to protect the initial login web applications and transaction authentication used to verify the authenticity of online transactions (Litan & Allan, 2006). The device enables users to extend their authentication infrastructure to implement transaction authentication without any additional hardware, software, or change in the user experience. It works by displaying details of each transaction, which the users can verify by entering the passwords and clicking a mouse.

Rapport protection technology

Rapport uses its vaults technology to defeat man in the browser attacks. Rapport controls communication and protects websites with API blocking between add-ons and the browser, when an add-on tries to perform an unauthorised operation such as read passwords or inject transaction during a session (Trusteer, n.d.).

Virtual Cryptogram

This is a virtual signing technology that uses the camera in the customer's mobile phone or a dedicated optical token. It removes the need for the awkward authenticators and time consuming re-keying of the challenge codes or the transaction

details. The large capacity allows more transaction details to be authenticated, and these can be changed rapidly, in response to adaptation in criminal behaviour (Cronto, 2008).

Privacy Configurations

The use of multi-protection approaches to guard online banking customers and Internet users is a more appropriate way to ensure security. It makes the customer's computer system more robust. The following tips are the privacy settings which can prevent customers from man-in-the-browser attacks, based on the author interest as a researcher and as an experienced online banking user who has had to deal with a range of phishing attacks.

- Install the anti-virus and the spyware, including the firewall applications on the computer and keep them up to date.
- Install the anti-browser toolbars that have ability to analyse the URLs, imagery on a site, text and various heuristics to ensure a safety of a website (Akwukwuma & Egwali, 2008).
- Back up all data before recover the system or modify any registry key.
- ***Disable or uninstall the suspicious add-ons features that may have been loaded or currently loaded by the IE, or run without requiring permission which including ActiveX Controls (see Figure 4).***
- If using Firefox, check Windows registry extension for any suspicious browser extension from the following directories:
    - `HKEY_CURRENT_USER\Software\Mozilla\Firefox\Extensions\`
    - `HKEY_LOCAL_MACHINE\Software\Mozilla\Firefox\Extensions\`
- If using IE, the directory is:
    - `HKCU\Software\Microsoft\Internet Explorer\Extensions\`
- If some names such as {08B0OSU-SGUOD-GU…} appear in the left column of Windows registry, then right click on each of them and click delete. It will remove the extensions from the browser.
- Uncheck all boxes that enable logging of browsing history and user entered strings to protect a hard disk recording, storing, and injecting.
- Remove cookies when exiting from the site and do not accept cookies at all.
- Always clear the private data when closing the browser (see Figure 5, if using Firefox).
- Uncheck remember passwords for sites.

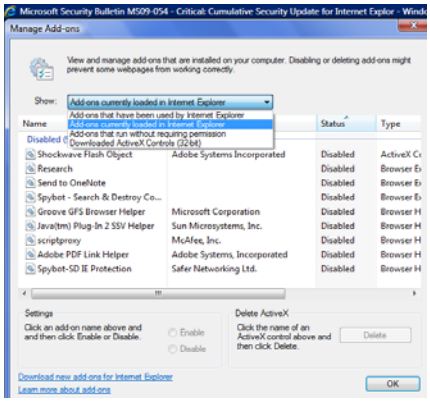


Figure 4 - Disable add-ons function in Internet Explorer

Figure 5 - Clear private data setting screen

Figure 6 - An example of a token security used in online banking authentication (Commonwealth Bank of Australia, n.d.)

Customer awareness

The best security to protect customers from the effects of browser Trojans is awareness. Banks or financial organisations, private security companies, governments, workplaces or academies can provide training, security protection knowledge, advertising campaigns, or basic knowledge of how to be safe while online.

- Customers should not permit any add-on components to be installed while they are surfing the Internet.
- Customers must check their bank account balances regularly and be aware of bank privacy policies and practices (US-CERT, 2008).
- Before performing any transactions, customers must thoroughly check the destination receiver of the account number, the name of the receiver, the amount of money and the date/time of sending.
- Customers must change their password every 3 to 6 months.
- Customers must not answer any email that asks for credential information or click the link provided.
- Customers should report any abnormal transaction activity to their bank, the police or other responsible crime investigators.
- If customers lose confidence in more conventional security providers, they should consider requesting a digital token security from their bank (see Figure 6 for an example of a token security).

They should also periodically consult with their bank on whether even better security technology has become available.

CONCLUSION

Man-in-the-middle browser add-on is formed as the Trojan browser extensions; poses a serious and growing threat to clients of online banking. Trojans operate by tricking customers into believing that they are an additional software component that can be used to facilitate the experience, particularly when customers use the browser to perform online transactions. Because the attacks work in real time, some standard computer security software cannot detect the Trojans. Internet security and transaction authentication protections are provided by private security companies and financial institutes to shield their customers from being attacked. Nevertheless, customers should also guard their computers by activating anti-Trojan and firewall protections to protect and detect all suspicious activities in their computer, and manually checking the browser configuration to ensure that the browser is set in a secure mode. Lastly, customer awareness is the most important thing that the customers should concern when accessing the Internet and they should follow the security guideline provided by banks or security forums on how to be safe when using online banking.

ACKNOWLEDGEMENT

The author specially thanks A/Prof Craig Valli for giving me the opportunity to write this paper and Dr. Judy Clayden and Dr. Greg Maguire for discussion and improving the writing style.

REFERENCES

Akwukwuma, V. V. N., & Egwali, A. O. (2008). E-Commerce: Online Attacks and Protective Mechanisms. *Asian Journal of Information Technology, 7*(9), 394-402.

Bayden Systems. (2004). TamperIE. Retrieved November 26, 2009, from http://www.bayden.com/TamperIE/

BitDefender. (2008). Trojan.PWS.ChromeInject.B. Retrieved October 30, 2009, from http://www.bitdefender.com/VIRUS-1000451-en--Trojan.PWS.ChromeInject.B.html

Blum, R., & LeBlanc, D.-A. (2009). *Linux for dummies*: For Dummies.

Blunden, B. (2009). *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System*: Jones & Bartlett Publishers.

Commonwealth Bank of Australia. (n.d.). An example of a token security used in online banking authentication: Commonwealth Bank of Australia.

Croll, A., & Power, S. (2009). *Complete Web Monitoring*: O'Reilly Media, Inc.

Cronto (2008). Beyond Phishing - De-Mystifiying The Growing Threat of Internet Banking Fraud. *Journal*. Retrieved from www.cronto.com/…/internet_banking_fraud_beyond_phishing.pdf

F-Secure Corporation. (2007). Trojan-Spy:W32/Nuklus.A. Retrieved October 21, 2009, 2009, from http://www.f-secure.com/v-descs/trojan-spy_w32_nuklus_a.shtml

Fadia, A. (2006). *The Unofficial Guide to Ethical Hacking Second Edition*: Thomson Course Technology.

Gühring, P. (2006). Concepts against Man-in-the-Browser Attacks. *Journal*. Retrieved from http://www2.futureware.at/future.htm

Hruska, J. (2008). New trojan targets Firefox, masquerades as Greasemonkey. Retrieved October 209, 2009, from http://arstechnica.com/security/news/2008/12/new-trojan-targets-firefox-masquerades-as-greasemonkey.ars

Ilett, D. (2006). Financial firms suffer most Trojan attacks. Retrieved September 26, 2009, from http://www.silicon.com/financialservices/0,3800010322,39157190,00.htm

Keizer, G. (2009). Sneaky Microsoft plug-in puts Firefox users at risk. Retrieved October 29, 2009, from http://www.computerworld.com/s/article/9139459/Sneaky_Microsoft_plug_in_puts_Firefox_users_at_risk

Krebs, B. (2006). Password-Stealing Trojan Disguised as Firefox Extension. Retrieved September 28, 2009, from http://blog.washingtonpost.com/securityfix/2006/07/passwordstealing_trojan_disgui.html

Leyden, J. (2008). Firefox plug-in Trojan harvests logins. Retrieved October 29, 2009, from http://www.theregister.co.uk/2008/12/04/firefox_plug_in_trojan/

Litan, A., & Allan, A. (2006). Transaction Verification Complements Fraud Detection and Stronger Authentication. Retrieved September 25, 2009, from http://www.tricipher.com/threats/man_in_the_browser.html

Louw, M. T., & Lim, J. S. (2008). Enhancing web browser security against malware extensions. *Journal in Computer Virology, 4*(3), 179-195.

Microsoft Corporation. (2009). Component Object Model Technology. Retrieved October 30, 2009, from http://www.microsoft.com/com/default.mspx

Oiaga, M. (2006). Internet Explorer BHO Trojan: Transmits stolen data via ICMP packets. Retrieved September 28, 2009, from http://news.softpedia.com/news/Internet-Explorer-BHO-Trojan-32403.shtml

Ollmann, G. (2009). 'Man-in-the-browser' Attack Vectors & Commercial Cyber-crime. *Journal*. Retrieved from www.zisc.ethz.ch/…/ETH2009-CommercialCyberCrime-GunterOllmann.pdf

Pogue, D. (2004). *Windows XP home edition: the missing manual*: O'Reilly Media, Inc.

Raffetseder, T., Kirda, E., & Kruegel, C. (2007). *Building Anti-Phishing Browser Plug-Ins: An Experience Report.* Paper presented at the 29th International Conference on Software Engineering Workshops(ICSEW'07).

Rietta, F. S. (2006). *Application Layer Intrusion Detection for SQL Injection*. Paper presented at the ACM SE. Retrieved October 21, 2009, from http://www.rietta.com/papers/rietta_acmse2006.pdf

RSA (2008). Mitigating Man-in-the-middle and Trojan Attacks: Best Practices for Combating Emerging Threats with Layered Security. *Journal*. Retrieved from www.rsa.com/products/securid/.../9528_MITM_WP_0708-lowres.pdf

Scambray, J., Shema, M., & Sima, C. (2006). *Hacking Exposed Web Applications Second Edition*. California: McGraw-Hill.

ScanSpyware. (2008). Nuklus.A. Retrieved October 21, 2009, from http://www.scanspyware.net/info/Nuklus.A.htm

SecurityMob. (2007). Infostealer.Nuklus. Retrieved October 21, 2009, from http://www.securitymob.com/my_smob/alert_info.asp?alert=55812

Ståhlberg, M. (2007). *The Trojan Money Spinner*. Paper presented at the Virus Bulletin Conference, Helsinki, Finland.

Trusteer. (n.d.). Man-in-the-Browser. Retrieved September 26, 2009, from http://www.trusteer.com/maninthebrowser

US-CERT. (2008). *Banking Securely Online*. Retrieved October 21, 2009. from http://www.us-cert.gov/reading_room/Banking_Securely_Online07102006.pdf.

Vugt, S. v. (2009). *Ubuntu Netbooks: The Path to Low-cost Computing*: Apress.

COPYRIGHT